

Application #09/646,640  
Amendment dated March 30, 2006

**Amendments to the claims:**

- 1        1. (previously cancelled)
- 2        2. (previously cancelled)
3. (previously cancelled)
4. (previously cancelled)
5. (previously cancelled)
6. (previously cancelled)
7. (previously cancelled)
8. (previously cancelled)
9. (previously cancelled)

- 1        10. (previously presented) Data protection method for operating a
- 2            microprocessor of a chip card to protect data elements contained in
- 3            a memory of a chip card from discovery by analysis of electrical
- 4            power consumption by the microprocessor, said method using a
- 5            cryptographic algorithm for executing operations for processing
- 6            said data elements so as to generate encrypted information, said
- 7            method comprising:
- 8                operating the microprocessor to randomly modifying the
- 9                    order of execution of operations involving
- 10                  manipulations of data elements contained in the
- 11                  memory from one cycle to another, a cycle being a
- 12                  complete execution cycle of the algorithm or an
- 13                  intermediate cycle of a group of operations, said
- 14                  operations being operations whose order of execution
- 15                  relative to the others does not affect the result,
- 16                  thereby protecting said data elements contained in
- 17                  said memory and processed by a microprocessor in a

Application #09/646,640  
Amendment dated December 28, 2005

- 18 chip card from discovery by analysis of the  
19 microprocessor's electric power consumption.
- 1 11. (previously presented) The protection method according to claim  
2 10, wherein the modified order of execution of operations include  
3 permutation of bits of a message block which is performed after the  
4 permutation of bits of a key, and vice versa.
- 1 12. (previously presented) The protection method according to claim  
2 10, wherein the modified order of execution of operations include a  
3 random determination of the processing of quartets.
- 1 13. (previously cancelled)
- 2 14. (cancelled)
- 1 15. (cancelled)
- 1 16. (previously presented) The data protection method of Claim 10  
2 wherein said data elements are keys.
- 1 17. (cancelled)